1

GIRARD SHARP LLP
Dena C. Sharp (State Bar No. 245869)
dsharp@girardsharp.com
Simon S. Grille (State Bar No. 294914)
sgrille@girardsharp.com
Nina R. Gliozzo (State Bar No. 333569)
ngliozzo@girardsharp.com
Jordan Isern (State Bar No. 343159)
jisern@girardsharp.com
601 California Street, Suite 1400
San Francisco, CA 94108
Telephone: (415) 981-4800
Facsimile: (415) 981-4846

2

3

4

5

6

7

8

9   *Attorneys for Plaintiffs*

10

11

12   UNITED STATES DISTRICT COURT

13   NORTHERN DISTRICT OF CALIFORNIA

14   SAN FRANCISCO DIVISION

15

16   VALERIE TORRES and RHONDA   Case No. 3:22-cv-07465-CRB
      HYMAN, individually and on behalf of all
17   others similarly situated,   **PLAINTIFFS' REPLY IN SUPPORT OF
                                             MOTION FOR CLASS CERTIFICATION**
18   Plaintiffs,
                                             Judge: Hon. Charles R. Breyer
19   v.   **Date: December 13, 2024**
                                             Time: 10:00 am
20   PRUDENTIAL FINANCIAL, INC.,   **Ctrm.:   Videoconference**
      ACTIVEPROSPECT, INC., and
21   ASSURANCE IQ, LLC,

22   Defendants.

23

24

25

26

27

28

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

1   **I.   INTRODUCTION**

2   There is no dispute that the Class meets all the requirements of Rule 23(a) here. Nor do

3   Defendants (Prudential Financial, Assurance IQ, and ActiveProspect) dispute that under Rule

4   23(b)(3), a class proceeding will be manageable and that it is the superior means of resolving this

5   litigation. Defendants do not challenge that classwide damages can be readily determined, as

6   CIPA provides for statutory damages. Defendants offer only two arguments against a finding of

7   predominance, contending that individualized inquiries will be required to determine whether

8   class members (1) gave implied consent and (2) have Article III standing. Defendants' arguments

9   misstate the applicable law, are unsupported by the evidence, and do not defeat certification.

10   Implied consent requires prior disclosure of the specific conduct being challenged, not (as

11   Defendants suggest) a general awareness of the possibility of interception. Given that

12   ActiveProspect's presence as a third party was undisclosed, consent could not have plausibly

13   been given here. Defendants cite some cases where the individualized nature of the implied

14   consent inquiry defeated predominance, but the defendant in those cases presented evidence that

15   the plaintiffs and many class members were already aware of the precise data collection practices

16   at issue there. This case is about the use of ActiveProspect's TrustedForm software—a type of

17   session replay technology that intercepted and recorded every class member's interactions with

18   Prudential's website in real time, divulging sensitive information, such as medical conditions.

19   Defendants offer news articles about session replay generally, law firm advertisements about

20   potential privacy violations on Prudential's website, Assurance's privacy policies, and their

21   expert's flawed survey—yet none of these sources explicitly or implicitly disclosed the use of the

22   TrustedForm software or show that even a single class member consented to what was occurring

23   on Prudential's website. Defendants' speculative argument fails under even their own cases.

24   Defendants' standing arguments fare no better, as they pertain not to standing, but to

25   identifying class members. But there is no administrative feasibility requirement, and whether a

26   class member was using a pseudonym or was in California when they used Prudential's webform

27   can be addressed through the claims process and verified through Defendants' records.

28   The requirements of Rules 23(a) and (b)(3) are met and the Court should certify the Class.

1   **II.   ARGUMENT**

2   **A.   The Issue of Implied Consent Does Not Defeat Predominance.**

3   **1.   Implied Consent Requires Disclosures That Would Have Put Class Members on Notice of Defendants' Conduct at Issue.**

4   CIPA requires that a defendant obtain knowing consent from all the participants before

5   intercepting communications. *See Gruber v. Yelp Inc.*, 55 Cal. App. 5th 591, 609 (2020), *as*

6   *modified on denial of reh'g* (Oct. 23, 2020). While CIPA allows for consent to be express or

7   implied, consent must be analyzed under a "reasonable person" standard, "any consent must be

8   actual," and "[t]o be effective, consent must be . . . to the particular conduct, or substantially the

9   same conduct." *Calhoun v. Google, LLC*, 113 F.4th 1141, 1147 (9th Cir. 2024) (citations omitted).

10 The circumstances must "convincingly show that the party knew about and consented to the

11 interception[.]" *Negro v. Superior Ct.*, 230 Cal. App. 4th 879, 892 (2014). Implied consent in this

12 case therefore requires "meaningful notice" that a class member's conversation would be intercepted

13 while looking on Prudential's website. *People v. Windham*, 145 Cal. App. 4th 881, 888 (2006).

14   "Courts have cautioned that implied consent applies only in a narrow set of cases" and

15 "consent should not be cavalierly implied." *In re Google Inc.*, 2013 WL 5423918, at *12 (N.D. Cal.

16 Sept. 26, 2013) (quotation marks and citation omitted). For example, implied consent was found

17 when a sign at a jail warned an inmate that calls there might be monitored and recorded. *Windham*,

18 145 Cal. App. 4th at 888. In another case, substantial evidence showed that the plaintiff consented to

19 her calls being recorded because, unlike here, the defendant's cardmember agreement explicitly

20 stated that "You agree that we may listen to and record phone calls between you and our

21 representatives" and during calls, a message stated that the calls "may be recorded," and the plaintiff

22 "participated in numerous calls . . . after receiving the prior recording disclosures." *Rojas v. HSBC*

23 *Card Servs. Inc.*, 93 Cal. App. 5th 860, 887 (2023), *review denied* (Nov. 21, 2023). Unlike in those

24 cases, Defendants never gave warning about the use of session replay on Prudential's website.

25   According to Defendants, implied consent will require case-by-case inquiries because it can

26 be inferred when class members "were aware of and expected third-party data collection on online

27 insurance sites," stressing a survey conducted by their expert. Opp. at 10. Defendants offer no

28 support for this contention, and it is not the law, as "knowledge of the *capability* of monitoring alone

- 2 -

1   cannot be considered implied consent." *Watkins v. L.M. Berry & Co.*, 704 F.2d 577, 581 (11th Cir.

2   1983) (emphasis in original). Circuit courts have held in the wiretapping context that consent cannot

3   be inferred just from an awareness of possible interception. Instead, there must be a prior disclosure

4   specific to that conversation. *See United States v. Staves*, 383 F.3d 977, 981 (9th Cir. 2004)

5   ("[F]oreseeability of monitoring is insufficient to infer consent."); *Berry v. Funk*, 146 F.3d 1003,

6   1011 (D.C. Cir. 1998) (awareness of the capacity to monitor calls is not the same as being told

7   "these *specific conversations* would be monitored") (emphasis added). As Judge Posner explained,

8   "knowledge and consent are not synonyms" so "[t]aking a risk is not the same thing as consenting to

9   the consequences if the risk materializes" and "[a] person who walks by himself late at night in a

10   dangerous neighborhood takes a risk of being robbed; he does not consent to being robbed." *United*

11   *States v. Daniels*, 902 F.2d 1238, 1245 (7th Cir. 1990). So the fact "[t]hat the person communicating

12   knows that the interceptor has the capacity to monitor the communication is insufficient to establish

13   implied consent." *In re Google Inc.*, 2013 WL 5423918, at *12 (N.D. Cal. Sept. 26, 2013); *see Ades*

14   *v. Omni Hotels Mgmt. Corp.*, 2014 WL 4627271, at *12 (C.D. Cal. Sept. 8, 2014) (that some class

15   members thought they might be recorded was not evidence of consent).

16   Moreover, consent to having a *third-party* intercept a user's communication on Prudential's

17   webform in real time cannot be inferred based only on an understanding that online insurance

18   sites—but not Prudential's—may collect data. There can be no implied consent where, as here, the

19   third-party's involvement was "invisible to the user[.]" *In re Pharmatrak, Inc.*, 329 F.3d 9, 21 (1st

20   Cir. 2003). There is no evidence that any class member knew that ActiveProspect was involved with

21   Prudential's website. Thus, even if there were evidence some class members were aware that

22   Prudential might have been using session replay technology on its site—and there is none—class

23   members still could not have given implied consent to ActiveProspect's eavesdropping.

24   Defendants' far-reaching reading of implied consent is not only contrary to the law but

25   would also lead to absurd results such as allowing businesses to engage in widespread wiretapping

26   and other privacy violations. When challenged, a business could invoke implied consent every time

27   a plaintiff had a vague notion that companies generally collect data online. *See Daniels*, 902 F.2d at

28   1245 (expressing "surprise[] at an argument that if illegal wiretapping were widespread anyone who

1   used a phone would have consented to its being tapped and would therefore be debarred from

2   complaining of the illegality."); *see also Berry*, 146 F.3d at 1011 (similar). It would also effectively

3   preclude a class action in any case where consent is a potential defense since a portion of any

4   putative class will likely have some familiarity with the risk of online surveillance. Courts have

5   repeatedly rejected sweeping readings of implied consent, and this Court should as well. *See In re*

6   *Google*, 2013 WL 5423918, at *14 (rejecting implied consent based on "theory . . . that all email

7   users understand and accept the fact that email is automatically processed" because it "would

8   eviscerate the rule against interception").

9   **2.   Defendants Have Not Shown That the Use of TrustedForm on Prudential's Website Was Common Knowledge.**

10   Based on their flawed characterization of what is sufficient to infer consent, Defendants

11   argue there are four sources "show[ing] that many class members knew about the alleged

12   interception" (Opp. at 11): (1) media reports; (2) advertisements from Plaintiffs' counsel; (3)

13   Defendants' privacy policies; and (4) Assurance's webform on other websites. Yet their showing

14   lacks evidence that a single class member received specific disclosures from these sources about the

15   use of TrustedForm on Prudential's website.[1] *See Ades*, 2014 WL 4627271, at *12 ("Despite

16   extensive discovery, Omni has not produced evidence that a single person meeting the class

17   definition actually consented to a call being recorded during the Class Period."). Without such

18   evidence, there is no reason to believe that any class member could have given implied consent to

19   Defendants' practices and unsupported arguments do not defeat predominance. *See True Health*

20   *Chiropractic, Inc. v. McKesson Corp.*, 896 F.3d 923, 932 (9th Cir. 2018) ("[W]e do not consider the

21   consent defenses [the defendant] might advance or for which it has presented no evidence.").

22

23

24

25   [1] Contrary to what Defendants argue, which side bears the burden of proof regarding consent at class certification is unsettled. *See Flowers v. Twilio, Inc.*, 2018 WL 10758024, at *3 (Cal. Super. Ct. Jan. 02, 2018) (granting class certification of CIPA claim but stating "[t]here is no controlling California case law regarding who has the burden of proof regarding consent under sections 631 and 632.7."). Recently in *Calhoun v. Google, LLC*, a case involving CIPA, the Ninth Circuit accepted the parties' consensus that consent was an affirmative defense. 113 F.4th 1141, 1147 (9th Cir. 2024). Regardless, Defendants have not shown that a significant portion of the class could have given implied consent.

26

27

28

1

2

    a. **There is No Evidence Any Class Member Learned About Defendants' Data Collection Practices Through News Articles or Law Firm Advertisements.**

3   Defendants speculate about the possibility that some class members may have learned about

4 the use of TrustedForm on Prudential's website from press coverage of this case and other lawsuits

5 involving session replay technology, as well as advertising from Plaintiffs' counsel. But the only

6 articles Defendants cite about *Javier*—a case involving an entirely different website—are from a

7 legal blog, the National Law Review, and JD Supra. *Compare* Defs.' Ex. 21 *with In re Google Inc.*

8 *Gmail Litig.,* 2014 WL 1102660, at *17 (N.D. Cal. Mar. 18, 2014) (noting widespread reporting on

9 Google's scanning of user accounts from the Houston Chronicle and Washington Post). The word

10 "Prudential" does not even appear anywhere in the articles Defendants cite, so a class member who

11 reviewed them would not have known about the same technology on Prudential's website.

12 Defendants also refer the Court to an article discussing this lawsuit (Defs.' Ex. 11) from a website

13 catering to "life insurers and annuity providers" that appeared on November 30, 2022, only two

14 weeks before the end of the class period (November 23, 2021 to December 13, 2022).[2]

15   Unlike the cases Defendants cite involving Google, where widespread coverage by the

16 mainstream press supported the inference that many class members likely consented to its conduct,

17 none of the articles Defendants cite here revealed the use of session replay technology on

18 Prudential's webform, and there is no evidence the typical consumer reads about the life insurance

19 and legal industries. Highlighting the unlikelihood that a reasonable consumer would have been

20 aware that their communications were being intercepted on Prudential's website is that even

21 Prudential's Global Chief Privacy Officer was unfamiliar with how TrustedForm works despite

22 being familiar with *Javier*, in which Prudential's subsidiary was a defendant. Gliozzo Reply Decl.,

23 Ex. 23 (Schmidt Dep. at 41:9-21) ("Q. What is your understanding of how TrustedForm functions? .

24 . . A. To the extent that it tracks compliance with TCPA. Q. How does it track compliance? A. I'm

25 not familiar with the specifics."); *id.* at 98:11-25 (familiar with *Javier* litigation).[3]

26

[2] https://www.lifeannuityspecialist.com/about (last visited November 5, 2024).

27

[3] The other news articles attached to Defendants' opposition are even less relevant as they just discuss session replay technology generally. For instance, articles from the BBC and Vice discuss

28 the technology but note that it was found on 480 out of the world's top 50,000 websites. Dkt. 81-21

Footnote continued on next page

1   The law firm advertisements Defendants have identified during the class period also would

2   not have put a reasonable consumer on notice, as these advertisements only advised consumers who

3   requested a quote from Prudential, "Your privacy may have been violated." *See* Defs.' Ex. 19 at 5.

4   None mentioned wiretapping or the use of session replay software. *See id.*; *see also* Defs.' Ex. 3

5   (Hyman Dep. at 21:17-22) (she saw an advertisement from Plaintiffs' counsel "along the lines of if

6   you've visited the Prudential website, your information may have been . . . inappropriately misused,

7   fill out this form for information."); Defs.' Ex. 4 (Torres Dep. at 26:3-10) (similar). These

8   statements do not "explicitly notify users of the conduct at issue," and do not defeat predominance.

9   *Calhoun*, 113 F.4th at 1147 (quotation marks and citations omitted).

10   While Defendants suggest the articles and advertisements put class members on inquiry

11   notice (Opp. at 10), they cite no authority showing that the standard applies in the consent context.

12   As this Court has noted, inquiry notice for statute of limitations purposes focuses on "knowledge of

13   *injury*." *Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891, 901 (N.D. Cal. 2023) (emphasis in

14   original). Implied consent, by contrast, turns on prior awareness of the specific conduct. In *Kearney*

15   *v. Salomon Smith Barney, Inc.*, the California Supreme Court rejected the lower court's statement

16   that consent under Penal Code section 632 may be inferred "even in the absence of an explicit

17   advisement" if a consumer had "reason to know" that their telephone calls were being recorded. 39

18   Cal. 4th 95, 118 n.10 (2006). Thus, the inquiry notice standard does not apply here, but even if it

19   does, the record still does not substantiate Defendants' predominance arguments because "courts

20   have found a plaintiff was on inquiry notice as to its claim based on publicly available information

21   [when] the information on which the defendant relied had been highly publicized." *In re Hard Disk*

22   *Drive Suspension Assemblies Antitrust Litig.*, 2022 WL 17096159, at *3 (N.D. Cal. Nov. 21, 2022).

23   That Prudential was using session replay technology on its website was not highly publicized, and

24   the coverage of the *Javier* litigation did not reveal Prudential's relationship with the other

25   defendants—which, for the reasons stated below, was not apparent, even to Plaintiffs' counsel—

26   _____

27   at 3, 7, 17. Another is an October 7, 2022 article—again shortly before the end of the class period—
about the pizza chain Papa John's being sued for using session replay software while another article
dated December 12, 2022 is about the cosmetics company Ulta Beauty. *Id* at 42, 51. None of the

28   articles concern the use of this type of technology on Prudential's website.

1   such that a reasonable consumer would suspect the use of similar technology when visiting

2   Prudential. *See Doe v. FullStory, Inc.*, 712 F. Supp. 3d 1244, 1256 (N.D. Cal. 2024) (CIPA claim

3   was timely when "[n]either article is so central to the conduct of . . . allegedly disclosing use of

4   defendants' tracking technology . . . to put plaintiff on inquiry notice.").

           b.   <u>**No "Empirical" Evidence Suggests That a Large Number of**</u>

5   <u>**Class Members Were Aware of Defendants' Practices.**</u>

6   Defendants attempt to bolster their consent argument with a survey conducted by their

7   expert, Dr. Nancy Mathiowetz, that purports to show that "a significant portion of potential class

8   members were aware of and expected third-party data collection on online insurance sites." Opp. at

9   10. Plaintiffs have moved to exclude the report and the survey under *Daubert* and Rule 702, but

10   irrespective of the outcome of that motion, the survey is not sufficiently tied to the facts of this case

11   to undermine predominance. *See also* Plaintiffs' Motion to Exclude; Gliozzo Reply Decl., Ex. 22

12   (John Rebuttal Rpt.), ¶¶ 14-44.

13   Defendants insist that the survey shows class members had divergent understandings of their

14   privacy (Opp. at 11), citing to *Brown v. Google LLC*, 2022 WL 17961497 (N.D. Cal. Dec. 12, 2022)

15   and *In re Google RTB Consumer Privacy Litigation*, 2024 WL 2242690 (N.D. Cal. Apr. 4, 2024).

16   But those cases are readily distinguishable, in part because the survey Dr. Mathiowetz conducted

17   here reveals nothing about consumers' understanding of Defendants' practices on Prudential's

18   website. *See* John Rebuttal Rpt., ¶¶ 18-22. In *Brown*, Google offered a survey about the alleged

19   interception and collection of data of Chrome browser users while in private (or incognito) browsing

20   mode. *See* 2022 WL 17961497, at *18. During the survey, Google's expert showed participants "the

21   documents plaintiffs claim comprise their contract" such as the incognito screen for Google's

22   browser and its privacy policies, and when presented with that information, respondents reported

23   expecting that "Google receives their IP addresses in Incognito mode, while 55% expect that Google

24   receives the URLs of sites visited and cookies." *Id.* In other words, the evidence showed that many

25   class members were aware of the precise practices at issue in the case. The defense expert in *Google*

26   *RTB* similarly tested respondents about their "expectations of its [Real Time Bidding] data

27   collection." 2024 WL 2242690, at *14.

28

1   In contrast to *Brown* and *Google RTB*, Dr. Mathiowetz's survey asked respondents if they

2   "were aware of third-party software on websites before taking the survey." Opp. at 11. That is not

3   evidence that any class member had the requisite prior understanding of what was occurring on

4   Prudential's webform. The figures from the survey are also significantly inflated and misleading for

5   several reasons, including that the survey's broad definition of "third-party software" lumps a

6   terminally vague description of session replay technology with software that generally collects and

7   stores user information on the website.[4] Mathiowetz Rpt. ¶¶ 50-57 & Figs. 9-13; John Rebuttal Rpt.

8   ¶ 27; *id.* ¶¶ 16-22; 24-43 (describing several bias-inducing elements in survey). This case is

9   therefore more similar to cases such as *Ades* where the court found that common issues

10   predominated despite the defendant's expert's "study" showing "half of California residents who

11   called 'business class or luxury hotels' within a recent one-year period assumed their calls were

12   recorded" because the study did not "show that any individual class members actually consented at

13   the time to their calls being recorded by [the defendant]." *Ades*, 2014 WL 4627271, at *11-12. In

14   *Flowers*, too, the court disagreed with the defendant's argument that implied consent was too

15   individualized because some users suspected their conversations might be recorded. 2018 WL

16   10758024, at *5. The court explained that "even if class members 'knew or had reason to know' that

17   their calls were being recorded, that would not necessarily establish consent" and did not

18   "undermine predominance of common issues" where there was no evidence that the defendant

19   disclosed that it would record their calls. *Id.*

20   **c.   Defendants' Privacy Policies Did Not Put the Class on Notice.**

21   Defendants also argue that individualized inquiries about implied consent will be necessary

22   because Prudential and Assurance's privacy policies gave notice of TrustedForm. These arguments

23   are again unsupported by evidence. Prudential's privacy policies would not have put Class members

24   on notice about the use of TrustedForm. To provide sufficient notice, "[t]he disclosures" in a privacy

25   policy "must have only one plausible interpretation for a finding of consent" and must "explicitly

26   notify users of the practice at issue." *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 620 (N.D. Cal.

---

27   [4] In addition, the framing of the survey primes respondents to assume consent was obtained for
the operation of the software or otherwise cues respondents to its operation (thus inflating their
28   reported awareness of it). John Rebuttal Rpt. ¶¶ 16-22.

2021) (cleaned up). Here, the privacy policies say nothing about third-party interception of user communications on Prudential's website. Mot. Exs. 15 and 16 (Prudential Privacy Notices); *see Valenzuela v. Kroger Co.*, 2024 WL 1336959, at *3 (C.D. Cal. Mar. 28, 2024) ("the Policy does not explicitly state that Kroger intended to route chats to third parties who would read, store, and harvest data from those chats."). In any event, regardless of whether Prudential's privacy policies provided sufficient notice, Defendants do not dispute that they were materially uniform across the class period and thus will generate a common answer. *See True Health*, 896 F.3d at 932 ("[T]here is little or no variation in the product registrations and the EULAs. For both of these asserted [consent] defenses, the predominance requirement of Rule 23(b)(3) is therefore satisfied."); *Flowers*, 2018 WL 10758024, at *5 (defendants "acted uniformly as to each class member" via posted privacy policy).

Defendants claim—without evidence—that a "significant number of class members" were likely aware their information was being intercepted because Prudential's webform, "Pru Branded Path" or "PBP," is similar to other Assurance webforms and Plaintiffs testified that they used other websites with Assurance's webforms. Citing this Court's final motion to dismiss order in *Javier v. Assurance IQ, LLC*, 2023 WL 3933070, at *2 (N.D. Cal. June 9, 2023), Defendants argue that the Court's holding that Assurance's privacy policy in *Javier* put the plaintiff on inquiry notice for statute of limitations purposes also put class members who visited Assurance websites on notice of similar monitoring on Prudential's website. Even overlooking that the inquiry notice standard is irrelevant here, Defendants are incorrect that the privacy policy on a separate website that is *not even openly affiliated with Prudential* informed consumers about Prudential's use of session replay on the webform. Neither the policy in *Javier* nor any subsequent versions of it, which Defendants tellingly did not provide the Court, revealed anything about the interception of their private data during the class period.

To start, nothing on the Prudential website gave any hint to users that the collection of their data on the webform would be governed by Assurance's privacy policies or even that Prudential's website used the same or similar software. During the class period, the webform exclusively had Prudential's branding, Prudential admits "a user on the website [would] have no reason to know that Assurance is involved at all" in its operation, and Assurance's privacy policies were never provided

1 to users. Mot. Ex. 10 (Renz Dep. at 104:9-19, 248:14-249:4). Where Assurance is mentioned at all,

2 Prudential's privacy policy specific to California consumers—the population relevant here—is

3 explicit that the "[d]isclosure is provided by Prudential Financial, Inc., its subsidiaries and affiliates,

4 *other than* Assurance IQ, LLC and its own subsidiaries." Mot. Ex. 16 (emphasis added).

5   The reverse is also true: nothing on Assurance's separate webforms or privacy policies

6 would tell users that its privacy policies also governed or were even related to the Prudential

7 webform at term.prudential.com. Defendants do not argue that either the Assurance privacy policy

8 or webforms advised visitors that Prudential's webform used the same wiretapping software,

9 because they did not. The version of Assurance's privacy policy in force during the class period says

10 its terms do not apply to Prudential: "'Assurance', 'we', 'us' and 'our' for purposes of this Privacy

11 Policy refers only to Assurance IQ, LLC and its subsidiaries, and [] not our parent company

12 Prudential Financial or any of its other subsidiaries." Gliozzo Reply Decl., Ex. 24 (Assurance

13 Privacy Policy) at 1. The 2019 version at issue in the *Javier* case similarly applies only to Assurance

14 by its own terms.[5] Nor do the Assurance webforms reveal any affiliation with Prudential, as they

15 bear different branding, for example, "National Family, [an] Assurance Corporation," and advise

16 consumers only that "This website is owned and operated by Assurance IQ, LLC, a licensed

17 insurance agency." *See* Gliozzo Reply Decl., Ex. 25 at 1.

18   Without substantiating evidence, Defendants' only argument is that Prudential's webform

19 was so similar to Assurance's other life insurance webforms that class members must have known

20 Prudential was using the same wiretapping technology as Assurance. While both webforms request

21 the same information, Prudential's Rule 30(b)(6) witness acknowledged "this is the information

22 necessary to generate a life insurance quote," Mot. Ex. 10 (Renz Dep. at 147:6-7), so visitors would

23 have no reason to assign significance to the similarity. There is only one mention of Prudential at all

24 on the Assurance webform, and it underscores that Prudential and Assurance are separate entities

25 such that consent is required for the sharing of private data between them. Ex. 25 at 2 ("I agree to

26

27 _____
   [5] *See Javier*, 3:20-cv-02860-CRB, Dkt. 58-2 at 4 (2019 Assurance Privacy Policy). Moreover,
   that policy was from before Prudential acquired Assurance in October 2019. *See* Dkt. 63

28 (Prudential Answer) ¶ 84.

1   Assurance sharing my information with Prudential companies and affiliates so that they can market

2   their products and services to me."); *see also* Defs. Ex. 16.

3   　　　The Court should reject Defendants' argument that these tenuous and vague connections

4   between Assurance's webform and Prudential are enough to impute implied consent to the operation

5   of TrustedForm on Prudential's webform.

6   　　　**3.　　Defendants' Own Cases Show That Implied Consent is Not an**
     　　　　　　　Obstacle to Class Certification.

7   　　　In focusing their arguments on implied consent, Defendants primarily rely on two cases,

8   *Brown* and *Google RTB*, where class certification was denied for wiretapping claims because of

9   implied consent, but the court's reasoning in each case shows that Defendants have not presented

10   sufficient evidence to substantiate their contention that implied consent will be individualized. In

11   *Brown*, a case about Google's alleged interception of user data while in private browsing mode, the

12   court relied on the defendant's evidence that among other things, "40% of named plaintiffs were

13   aware of media and academic reports discussing the privacy limitations of private browsing mode."

14   2022 WL 17961497, at *18. Another plaintiff testified he was aware of a developer tool that

15   revealed whether data was being collected while in private mode. *Id.* In *Google RTB*, the record

16   showed widespread media coverage about Google's RTB practice of disclosing user information

17   and that many users were familiar with Google's disclosures about its data sharing practices. 2024

18   WL 2242690, at *13-14. These and the other cases Defendants cite suggest that individual issues

19   may predominate where the defendant puts forth evidence that many class members were aware of

20   the defendant's specific data practices.[6]

21   　　　Defendants have made no similar showing here. Despite ample discovery, there is no sign

22   that any class member was aware of Defendants' use of TrustedForm on Prudential's webform. *See*

23   *Campbell v. Facebook Inc.*, 315 F.R.D. 250, 266–67 (N.D. Cal. 2016) ("While Facebook does

24

25   [6] In another one of Defendants' cited cases, it was "undisputed" that the defendant's practices were
26   disclosed by its privacy policy, on "iOS App's Privacy Settings page", and in "a number of published
     news articles[.]" *Hart v. TWC Prod. & Tech. LLC*, 2023 WL 3568078, at *11 (N.D. Cal. Mar. 30,
27   2023); *see also Backhaut v. Apple Inc.*, 2015 WL 4776427, at *14 (N.D. Cal. Aug. 13, 2015) (noting
     the defendant's "disclosures on its website regarding iMessage" and that the plaintiffs themselves "put
28   forth evidence of widespread publicity regarding the iMessage issue").

1   invoke implied consent as a defense that could potentially raise individual issues, based on the

2   current state of the evidence, those individual issues remain just that—potential."). Unlike in *Brown*,

3   2022 WL 17961497, at *18, where many named plaintiffs admitted familiarity with reports about

4   Google's disputed practices, both Plaintiffs testified that they were unaware of (and did not consent

5   to) the use of TrustedForm on Prudential's website. Gliozzo Reply Decl., Ex. 26 (Torres Dep. at

6   207:4-18); Ex. 27 (Hyman Dep. at 205:13-206:13). In further contrast to both cases, the disclosures

7   in the articles and advertisements Defendants cite were not specifically about Prudential's website,

8   and the survey they offer is also not sufficiently tied to their alleged conduct. While in *Google RTB*,

9   the defendant's practices were disclosed in its privacy policy, the use of session replay software here

10   was not disclosed in Defendants' privacy policies. 2024 WL 2242690, at *12-13.

11   Courts have consistently held that implied consent does not defeat predominance where, as

12   here, the defendant fails to present evidence that the challenged practice was well known to the

13   wider public. In *Campbell*, "news reports" specifically discussing one of Facebook's challenged

14   practices rendered claims based on the practice unsuitable for class treatment, but the court reached

15   a different conclusion about other challenged Facebook practices for which no similar evidence was

16   presented. 315 F.R.D. at 266-67. Other courts are in accord, rejecting similar consent arguments at

17   class certification as unsubstantiated and speculative. *See Flowers*, 2018 WL 10758024, at *5

18   ("Defendant has not offered individual testimony of any class member, or, other than speculation,

19   made a showing that individual class member testimony [about consent] is likely to play a

20   significant part in the trial of this case.") (citing *Ades¸* 2014 WL 4627271, at *12).

21   The Court should reach the same conclusion here. This is not a case involving Google or

22   Facebook—two of the largest and most widely covered companies in the world—where the universe

23   of information available to consumers about their data collection practices is enormous. The record

24   does not include *evidence* that class members were aware of what was occurring when they visited

25   Prudential's website, and implied consent does not defeat predominance.

26   **B.   Determining Class Member Standing Will Not Require Individual Inquiries.**

27   Defendants also insist that ensuring class members have Article III standing will require

28   individualized inquiries over whether a member had their personal information intercepted while

- 12 -

1   they were in California. Opp. at 11-12 (citing *TransUnion LLC v. Ramirez*, 594 U.S. 413, 431

2   (2021)). These arguments concern identifying class members, which is not grounds for denying

3   class certification. *See Zakinov v. Ripple Labs, Inc.*, 2023 WL 4303644, at *6 (N.D. Cal. June 30,

4   2023) (citing *Briseno v. ConAgra Foods, Inc.*, 844 F.3d 1121, 1126 (9th Cir. 2017)).[7]

5
         1.   **Whether Information in Defendants' Database Corresponds With Individuals With a CIPA Claim Can be Addressed Through the**
6   **Claims Process.**

7   Defendants argue that because some users may have obtained life insurance quotes for

8   others, they may have entered someone else's personal information so "the information in the

9   database for the PBP do not correspond to individuals with a potential claim." Opp. at 12-13. This is

10   not a predominance problem because "Class members who are not entitled to damages may be

11   weeded out at the claims phase[.]" *Utne v. Home Depot U.S.A., Inc.*, 2022 WL 1443338, at *8 (N.D.

12   Cal. May 6, 2022); *see also Kellman v. Spokeo, Inc.*, 2024 WL 2788418, at *11 (N.D. Cal. May 29,

13   2024) (issues with determining whether someone was a class member did not defeat class

14   certification when they could be "screened out"); *Trevino v. Golden State FC LLC*, 2023 WL

15   3687377, at *26 (E.D. Cal. May 26, 2023) (same).

16   Here, too, confirming that a person who filled out the webform is the same one submitting a

17   claim can be done through the claims process using Defendants' records. The example Defendants

18   cite involving Plaintiff Hyman is instructive. Hyman requested a life insurance quote on behalf of

19   her father on nationalfamily.com, which is also run by Assurance, but she also provided her own

20   email address and phone number. Defs. Ex. 16; Gliozzo Reply Decl., Ex. 27 (Hyman Dep. at 92:10-

21

22   ―――――――――――――
[7] The Ninth Circuit has explained that privacy violations have long been actionable under the common law and "California legislature intended to protect these historical privacy rights when [it]

23   passed . . . CIPA." *In re Facebook Inc. Internet Tracking Litigation*, 956 F.3d 589, 598 (9th Cir. 2020). CIPA thus codifies a substantive right to privacy "which causes concrete harm any time there

24   is a violation." *Campbell v. Facebook, Inc.*, 951 F.3d 1106, 1119 n.8 (9th Cir. 2020) (cleaned up); *see James v. Walt Disney Co.*, 701 F. Supp. 3d 942, 949 (N.D. Cal. 2023) (*TransUnion* did not

25   "gut[]" the holding of *In re Facebook*); *Brooks v. Thomson Reuters Corp.*, 2023 WL 9316647, at *6 (N.D. Cal. Aug. 10, 2023) (same). Moreover, that the Class may include some uninjured members

26   is not an obstacle to class certification. *Olean Wholesale Grocery Coop., Inc. v. Bumble Bee Foods LLC*, 31 F.4th 651, 669 (9th Cir. 2022) (en banc); *see also Gunaratna v. Dennis Gross Cosmetology

27   LLC*, 2023 WL 5505052, at *21 (C.D. Cal. Apr. 4, 2023) ("*TransUnion* does not require that

28   Plaintiffs' *prove* standing as to all members of the class[.]") (emphasis in original).

15). Using that contact information, Defendants identified from their own records that Plaintiff

Hyman, not her father, submitted the form on Assurance's other website. Similarly, here, absent

class members can be identified using a combination of the names and the contact information they

provided when submitting the Prudential webform. Mot. Ex. 10 (Renz Dep. at 114:17-21)

(Assurance's database contains all contact information provided on webform). If any class member

submitted the webform using another name, they could still be identified using the email address

and/or phone number provided and can attest during any claims process that the submission is theirs.

2.   Defendants' Records Can Identify California Users.

Defendants argue that "IP addresses do not necessarily indicate an individual's location

when accessing a particular website" because of the use of VPNs and proxy servers. Opp. at 13. A

user's IP address can be cross-referenced with the zip code they submitted on their webform, and

Plaintiffs need not identify class members to certify a class. *Williams v. Apple, Inc.*, 338 F.R.D. 629,

645 (N.D. Cal. 2021) (difficulties in identifying class members "is no bar to predominance");

Chinitz v. Intero Real Est. Servs., 2020 WL 7391299, at *14 (N.D. Cal. July 22, 2020). In any event,

Defendants' insistence that a California IP address cannot be a reasonable proxy for being in

California is simply not credible. Even though each class member provided their zip code on the

webform, Defendants opted to use IP address to identify California submissions, and Prudential's

corporate designee agreed that using a California IP address "was [the] best proxy available for

whether folks were in California." Gliozzo Reply Decl., Ex. 28 (Renz Dep. at 116:4-20). In an

interrogatory seeking to quantify the number of class members who submitted the webform while in

California, Prudential also provided the number of individuals who submitted the webform from a

California IP address. Gliozzo Reply Decl., Ex. 29 (Prudential Resp. to Interrogatories 1 and 2);

Mot. Ex. 10 (Renz Dep. at 112:11-113:6). In other words, until class certification, Defendants have

agreed that a California IP address is a reasonable proxy for user location.

The VPN data Defendants cite does not create individualized issues that will predominate

here. Defendants' survey expert noted that most people who use VPNs do so for their job and not in

their personal internet use and she even had to adjust the wording of the survey to attempt to isolate

personal VPN use. *See* Mathiowetz Rpt., Dkt. 81-8 at 80. Moreover, if, as Dr. Mathiowetz's survey

1   testing observed, respondents answered based on their professional use in addition to personal use,

2   the survey likely overreports the number of class members who may have been using a VPN while

3   submitting the webform.

4   Defendants also rely on another expert, Dr. Nathaniel Polish, but his opinions are at most

5   speculative as he readily acknowledges that IP address generally is a good indicator of physical

6   location, arguing only that it is not "necessarily" true that IP address and location match. Polish

7   Decl., ¶ 9, Dkt. 81-24. Polish does not state that a VPN necessarily reports a *different* location than

8   the user's actual location and Defendants make no effort to quantify the number of people whose

9   actual location and VPN IP address location would be mismatched. Thus, even if a small portion of

10   class members used a VPN while submitting the form—and Defendants have not identified a

11   specific number—many may have still been within California at the time.

12   The court in *Svoboda v. Amazon.com, Inc*. rejected similar arguments that IP addresses are

13   insufficient to identify class members in a particular state, holding that a combination of billing

14   address and IP address location data "will identify persons who used the [technology at issue] while

15   in Illinois, and claim-form affidavits can serve as an additional cross-check." 2024 WL 1363718, at

16   *10 (N.D. Ill. Mar. 30, 2024). As in *Svoboda*, a class member's presence in California when the

17   webform was submitted can be "cross-check[ed]" through claim-form affidavits. *Id.* The zip code

18   that class members gave when submitting the form is also available in the dataset to provide an

19   additional cross-check. *Id.*; *see also Larsen v. PTT, LLC,* 2024 WL 4481216, at *3 (W.D. Wash.

20   Apr. 17, 2024).

21   **III.   CONCLUSION**

22   For all these reasons and the reasons stated in their Motion for Class Certification, Plaintiffs

23   request that the Court certify the Class and appoint them as class representatives, appoint Girard

24   Sharp LLP as class counsel, and direct the parties to submit a proposed plan of notice.

25

26   Dated: November 8, 2024   Respectfully submitted,

27   **GIRARD SHARP LLP**

28   */s/   Nina R. Gliozzo*

Dena C. Sharp (State Bar No. 245869)
dsharp@girardsharp.com
Simon S. Grille (State Bar No. 294914)
sgrille@girardsharp.com
Nina R. Gliozzo (State Bar No. 333569)
ngliozzo@girardsharp.com
Jordan Isern (State Bar No. 343159)
jisern@girardsharp.com
601 California Street, Suite 1400
San Francisco, CA 94108
Telephone: (415) 981-4800
Facsimile: (415) 981-4846

Attorneys for Plaintiffs

PLAINTIFFS' REPLY ISO MOTION FOR CLASS
CERTIFICATION
CASE NO. 3:22-CV-07465-CRB

1
<u>CERTIFICATE OF SERVICE</u>

2
  I hereby certify that on November 8, 2024, I electronically filed the foregoing document

3
with the Clerk of the Court using the CM/ECF system, which will automatically send notification

4
of the filing to all counsel of record.

5
              By: /s/ *Nina R. Gliozzo*

6
                 Nina R. Gliozzo

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

PLAINTIFFS' REPLY ISO MOTION FOR CLASS
CERTIFICATION
CASE NO. 3:22-CV-07465-CRB